REMARKS

Claims 1, 10, 16, 21 and 24 are proposed for amendment herein. Claims 1-3, 6-12, 14-24 and 26-27 are presently pending in the above-identified application.

Applicants wish to thank the Examiner for carefully considering Applicants' prior request for reconsideration and withdrawing the finality of the rejection set forth in the prior Office Action.

With respect to the current Office Action and new grounds of rejection, Applicants present this Amendment that contains a response to the outstanding rejections and amends the independent claims to more particularly claim the invention.

Applicants respectfully submit, in view of this Amendment, that each of the currently pending claims, as amended, is patentably distinct from the cited prior art and in condition of allowance.

Rejection of Claims under 35 USC § 102(e)

The Office Action rejected claims 1-3, 6-12 14-24 and 26-27 under 35 USC § 102(e) as being anticipated by U.S. Patent No. 6,725,378 issued to C. Schuba et al. (hereinafter "Schuba"). Applicants have amended the independent claims herein to more particularly claim the various aspects of the invention, and respectfully submit that each of the currently pending is patentably distinct from Schuba.

As discussed in prior Amendments (and the Appeal Brief) in the present application, Applicants' claimed invention is directed at ascertaining the integrity of a communications network and thereby identifying potential security risks across the perimeter of such network. Thus, an aspect of the invention is directed to the determination of a security characteristic of a host (or hosts) associated with a first communications network wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host (associated with a first network) is probed with a particular packet, where the packet is intentionally configured with a source address which is associated with the second communications network, and the connectivity measure is determined as function

BEST AVAILABLE COPY

of a response from the probed host (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, lines 20-22) to the packet.

Importantly, the probe packet used in the present invention is generated and transmitted in particular fashion to take advantage of the principles of the invention. In particular, the source address is selected such that the IP address is external to the probed host's network, that is, the originator address is "false or derived" in that it does not originate from an actual host request (see, e.g., Applicants' Specification, page 9, lines 25-29). Thus, in accordance with claimed invention, as more particularly set forth in the amended independent claims herein, the generation of the probe packet is instrumental in that the source address is selected independent of any request from the second host to the first host. Thus, by generating the particular packet and probing the connectivity of the particular host(s) within a network using such generated packets, in accordance with the claimed invention, an analysis of the network can be made to identify potential security risks across the perimeter of the particular network.

Said another way, Applicants' claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to a specifically generated, configured and transmitted probe packet. This is in contrast to known so-called "self-defending networks" which may employ filtering techniques within a network to limit the amount and type of Internet protocol messages allowed to by exchanged through a network at any one time (see, Applicants' Specification page 3, line 24 through page 4, line 2). Indeed, Applicants submit that Schuba is one example of such known techniques, as detailed hereinbelow.

In brief, it is the determination of such connectivity measure, using the probe packet--generated and configured in accordance with the invention--that is the contribution advanced by the Applicants over the cited prior art. Applicants have realized that spoofed packets can serve different purposes (and non-malicious) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by system administrators to identify potential security risks across a network's perimeter and prevent malicious attacks (including but not limited to malicious spoofing).

Applicants have amended the pending independent claims to more particularly claim the above-described aspects of the invention. For example, amended independent claim 1 recites:

"A communications network security method for ascertaining the integrity of a first communications network and identifying potential security risks across a perimeter of the first communications network, the method comprising:

identifying a plurality of routes that define the first communications network;

identifying a plurality of hosts associated with the first communications network as a function of the plurality of routes;

receiving a census of the first communications network as a function of the plurality of hosts to determine a topology of the first communications network;

probing at least one first host of the plurality hosts of the first communications network by ***generating*** and transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a source address of a second host which is associated with a second communications network, wherein the source address is selected independent of any request from the second host to the first host; and

determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network, the measure of connectivity being an indication of connectivity between the first communications network and the second communications network." (emphasis added by Applicants)

Each of the currently pending independent claims has been amended in a similar fashion as the above-referenced amended independent claim 1 to contain similar limitations directed to the above-described features of the invention.

It is at least the above-described aspects of Applicants' invention that stand in contrast to Schuba. Applicants appreciate how the Examiner may have found certain similarities between Schuba and Applicants disclosed invention in that the two are directed at network security. However, Schuba does not anticipate, teach or suggest the aspects of Applicants invention as set forth above. As cited and referenced in the Office Action, Schuba's technique incorporates a so-called "monitor" that is arranged to capture IP/TCP datagrams passing along a network (see, e.g., Schuba, column 7, lines 38-41). However, Schuba's monitor does not generate probe packets as required by Applicants claimed invention. Rather, the monitor utilizes a database (see, e.g., Schuba, column 8, lines 5-10; and FIG. 3 element 57 – "database") containing three categories of addresses: "acceptable", "unacceptable", and "suspect" (see, e.g., Schuba, column 8, lines 18-47; column 3, lines 8-10; and column 11, lines 9-15) to analyze already transmitted packets and classify such packets/messages in accordance with the database content.

Schuba's technique requires classification of TCP packets into one of the aforementioned categories in order to implement the filtering technique and security measure taught by Schuba. This is in contrast to Applicants' claimed invention which generates a particular packet, configured in a specific fashion, to identify potential security risks across the perimeter of such network. Therefore, Applicants claimed invention as set forth in the amended claims herein is patentably distinct from and over Schuba and Applicants respectfully request that any such rejection be withdrawn.

Regarding the rejection of each of the presently pending dependent claims these claims depend ultimately from one of the pending amended independent claims 1, 10, 16, 21 and 24 herein which Applicants submit are patentably distinct over Schuba for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Schuba for the aforesaid reasons, as well as other elements these claims add in combination to their base claim.

Rejection of Claims under 35 USC § 112

As mentioned above, Applicants acknowledge the withdrawing of the finality of the rejection set forth in the prior Office Action. As such, Applicants are somewhat confused by the continued rejection of claims 1, 7, 10, 16, 20, 21, 23 and 24 under 35 USC § 112, first paragraph. Perhaps this was merely an inadvertent error by the Examiner. However, if not, Applicants again traverse the rejection as follows:

Claims 1, 10, 16, 21 and 24

The Office Action rejected claims 1, 10, 16, 21 and 24 under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement, in particular, with respect to the claimed "security characteristic" and "an indication of connectivity" subject matter. In so rejecting such claims, the Examiner asserts (see, Office Action, page 6) that "the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention."

With respect to the claimed "security characteristic" subject matter, such subject matter is supported and described in at least the following passages in Applicants' Specification: (i) page 4, lines 22-30; (ii) page 8, lines 1-11; (iii) page 10, line 5-28; (iv) page 6, lines 10-26; and (v) page 5, lines 1-6. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "security characteristic" of Applicants' invention is directed to identifying potential security risks across the perimeter of a network (see, e.g., Applicants' Specification, page 4, lines 27-30; and page 8, lines 17-22) which, in turn, is the "determining a security characteristic of the probed host" as claimed by Applicants. Examples of such security risks will be appreciated by those skilled in the art, and Applicants set forth a number of such exemplary security risks in their Specification at page 2, line 28 through page 3, line 10; and page 1, line 28 through page 2, line 10. That is, the security characteristic of the probed host, in accordance with the invention, is whether such probed host poses a security risk across the perimeter of the associated network. This feature of the invention is supported by the above-referenced passages of Applicants' Specification in enabling

one skilled in the art to make and/or use the claimed security aspects of Applicants' claimed invention.

With respect to the claimed "an indication of connectivity", such subject matter is supported and described in at least the following passages of Applicants' Specification: (i) page 5, lines 1-6; (ii) page 5, lines 26-29; (iii) page 8, lines 1-22; (iv) page 9, line 15 through page 11, line 14; and (v) FIG. 2. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "indication of connectivity" of Applicants' invention is directed at discovering connectivity of, or between, a host machine (or host machines) as a function of a response (or absence thereof) to the specifically configured probe packet. As will be recognized by one skilled in the art the "connectivity" aspect of the claimed invention is the existence of, or absence of, a connection. This feature of the invention is supported by the above-referenced passages of Applicants' Specification in enabling one skilled in the art to make and/or use the security aspects of Applicants' claimed invention.

Regarding the Examiner's questions on page 6 of the Office Action: (i) "...it is not clear what is being measured regarding the security characteristic..."; and (ii) "Is the measure of indication of connectivity pertains to available bandwidth, traffic load, or the integrity of the network?" It will be appreciated from Applicants' Specification, as detailed above, that the claimed "indication of connectivity" is directed to the existence of, or absence of, a connection. Thus, in accordance with the claimed invention, the "measure" is the existence (or absence of) the connection itself. The particular attributes of such connection (e.g., bandwidth or traffic load) as raised by the Examiner are irrelevant in terms of the claimed invention and do not serve as proper grounds for rejecting Applicants claims under §112, first paragraph. The relevant aspect with regard to the claimed invention is the existence of, or absence of, a connection as clearly indicated by the pending claims and supported by Applicants' Specification.

For the reasons discussed above, the terms "security characteristic" and "an indication of connectivity" comply with the requirements of §112, first paragraph and Applicants respectfully request reversal of the §112, first paragraph rejections thereof.

Claims 7, 20 and 23

The Office Action separately rejected claims 7, 20 and 23 under 35 USC § 112, first paragraph, as failing to comply with the enablement requirement, in particular, with respect to the claimed "different security levels". In so rejecting such claims, the Examiner asserts (see, Office Action, page 6) that "the claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected or with which it is most nearly connected, to make and/or use the invention".

With respect to the claimed "different security levels", such subject matter is supported in at least the following passages of Applicants' Specification: (i) page 8, lines 5-11; (ii) page 10, lines 5-20; (iii) page 6, lines 1-9; and (iv) page 6, lines 10-26. At a minimum, such passages from Applicants' Specification enable one skilled in the art to recognize that the claimed "different security levels" aspect of Applicants' invention is directed to ascertaining the security of different types of networks, e.g., an intranet vs. the Internet, or a corporate backbone vs. an external network. One skilled in the art will clearly recognize that such disparate networks may have "different security characteristics" which are well-known and typically specified by the network's system administrators. For example, the computer network security characteristics which are addressed by such network administrators include the examples of the types of security threats detailed in Applicants' Specification beginning on page 1, line 25 and continuing at least through page 4, line 16. Such varying security characteristics together with well-known network types (e.g., intranets, Internet, private networks, public networks, etc.) will be readily apparent to those skilled in the art, and in addition to the descriptions of such aspects of the claimed invention in Applicants' Specification, will enable one skilled in the art to make and/or use such claimed invention.

Regarding the Examiner's question on page 3 of the instant Office Action: "Does different security levels means access authentication for users, or security policy implemented on the network in general and on firewall in particular?" It will be appreciated from Applicants' Specification, as detailed above, that the claimed "different

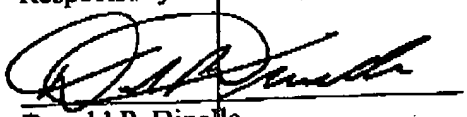
security levels" between the first and second networks is directed to the most basic of principles, that is, that the first and second networks have differing (i.e., not the same; dissimilar; distinct; or separate) security levels. For example, as will be readily appreciated by those skilled in the art, a private network and public network will have differing needs with respect to security levels. That is, the degree of the differing security levels (or the specific implementation or delivery of thereof) is not the focus of the claimed invention. Rather, the relevant aspect with regard to the claimed invention, as recited in claims 7, 20, and 23, is that the first and second communications network have different security levels.

For the reasons discussed above, the "different security levels" as claimed by Applicants complies with the requirements of §112, first paragraph and Applicants respectfully request reversal of the §112, first paragraph rejections.

Therefore, in view of the foregoing, Applicants respectfully submit that each of the currently pending claims, as amended, is patentably distinct from Schuba. As such, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Donald P. Dinella
Attorney for Applicant(s)
Reg. No. 39, 961
(908) 582-8582

Date: December 28, 2006

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.